(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 858 296 A3**

(12) **EUROPEAN PATENT APPLICATION**

(88) Date of publication A3:
02.09.2015 Bulletin 2015/36

(43) Date of publication A2:
08.04.2015 Bulletin 2015/15

(21) Application number: **14179107.9**

(22) Date of filing: **30.07.2014**

(51) Int Cl.:
H04L 9/00 *(2006.01)*

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME

(30) Priority: **07.08.2013 JP 2013163793**

(71) Applicant: **FUJITSU LIMITED**
Kawasaki-shi,
Kanagawa 211-8588 (JP)

(72) Inventors:
- **Yasuda, Masaya**
  Kanagawa, 211-8588 (JP)
- **Shimoyama, Takeshi**
  Kanagawa, 211-8588 (JP)
- **Kogure, Jun**
  Kanagawa, 211-8588 (JP)

(74) Representative: **Hoffmann Eitle**
Patent- und Rechtsanwälte PartmbB
Arabellastraße 30
81925 München (DE)

(54) **Information processing technique for secure pattern matching**

(57) An encrypted first polynomial that is obtained by encrypting, in a homomorphic encryption method that handles a polynomial processing, a first polynomial, is received from another computer. The first polynomial is represented by using, as coefficients, components of a first binary vector generated from first data in first order that is either ascending order or descending order with respect to degree of the first polynomial. Then, a predetermined processing in an encrypted text space is performed by using the encrypted first polynomial and an encrypted second polynomial that is obtained by encrypting a second polynomial in the homomorphic encryption method. The second polynomial is represented by using, as coefficients, components of a second binary vector generated from second data in second order that is different from the first order with respect to degree of the second polynomial. Then, a result of the predetermined processing is sent back.

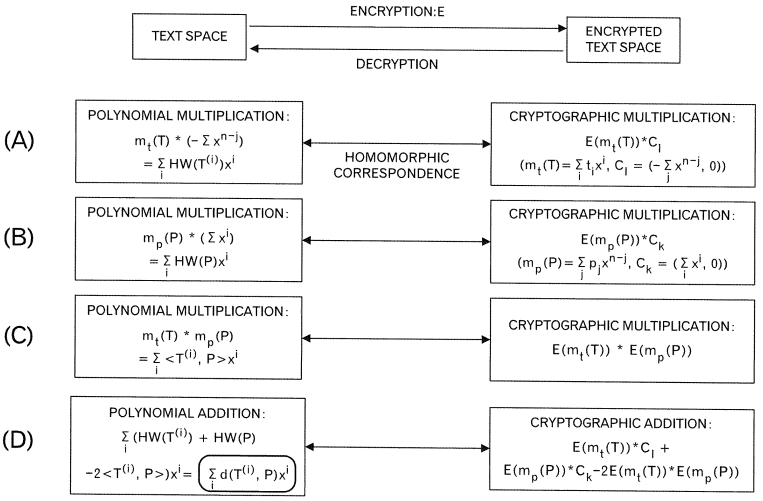

FIG.2

EP 2 858 296 A3

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 14 17 9107

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X,P	MASAYA YASUDA ET AL: "Secure pattern matching using somewhat homomorphic encryption", CLOUD COMPUTING SECURITY WORKSHOP, ACM, 2 PENN PLAZA, SUITE 701 NEW YORK NY 10121-0701 USA, 8 November 2013 (2013-11-08), pages 65-76, XP058034246, DOI: 10.1145/2517488.2517497 ISBN: 978-1-4503-2490-8 * paragraph [0002] - paragraph [0003] *	1-8	INV. H04L9/00
X	YASUDA MASAYA ET AL: "Analysis of Lattice Reduction Attack against the Somewhat Homomorphic Encryption Based on Ideal Lattices", 13 September 2012 (2012-09-13), ADVANCES IN COMMUNICATION NETWORKING : 20TH EUNICE/IFIP EG 6.2, 6.6 INTERNATIONAL WORKSHOP, RENNES, FRANCE, SEPTEMBER 1-5, 2014, REVISED SELECTED PAPERS; [LECTURE NOTES IN COMPUTER SCIENCE , ISSN 1611-3349], SPRINGER VERLAG, DE, PAGE(S) 1 - 16, XP047037754, ISSN: 0302-9743 ISBN: 978-3-319-21667-6	1,7,8	
Y	* paragraph [0002] *	2-6	
	-/--		

TECHNICAL FIELDS SEARCHED (IPC)
H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	27 July 2015	Bec, Thierry

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 14 17 9107

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
Y	LAGENDIJK R L ET AL: "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation", IEEE SIGNAL PROCESSING MAGAZINE, IEEE SERVICE CENTER, PISCATAWAY, NJ, US, vol. 30, no. 1, 1 January 2013 (2013-01-01), pages 82-105, XP011505535, ISSN: 1053-5888, DOI: 10.1109/MSP.2012.2219653 * page 90 - page 96 * -----	2-5	
Y	JOSHUA BARON ET AL: "5PM: Secure Pattern Matching", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20121219:161334, 12 December 2012 (2012-12-12), pages 1-77, XP061007031, [retrieved on 2012-12-12] * paragraph [0001] - paragraph [0003] * -----	6	
			TECHNICAL FIELDS SEARCHED (IPC)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	27 July 2015	Bec, Thierry

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)